WHAT IS CLAIMED IS:

1. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:

transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy;

transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued; and

blocking Internet access for any client computer that does not respond appropriately to said challenge.

2. The method of claim 1, wherein a client computer that does not respond at all is blocked from Internet access.

3. The method of claim 1, wherein a client computer that responds with a particular predefined code indicating non-compliance is blocked from Internet access.

4. The method of claim 1, wherein a client computer that responds with a particular predefined code indicating compliance is permitted Internet access.

5. The method of claim 1, further comprising:

before receipt of a challenge, transmitting an initial message from a particular client computer to the client premises equipment, for requesting the client premises equipment to transmit a challenge to that particular client computer.

6. The method of claim 5, wherein said initial message comprises a "client hello" packet.

7. The method of claim 1, wherein said client premises equipment is capable of permitting Internet access by selected client computers and denying access to other client computers.

8. The method of claim 1, wherein said access policy specifies rules that govern Internet access by the client computers.

9. The method of claim 1, wherein said step of blocking Internet access includes:

determining whether permitting Internet access for a given client computer would violate any of said rules, and

if permitting such Internet access would violate any of said rules, denying Internet access for that client computer.

10. The method of claim 1, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

11. The method of claim 1, wherein said access policy specifies which applications are allowed Internet access.

12. The method of claim 1, wherein said access policy specifies applications that are allowed Internet access.

13. The method of claim 12, wherein said applications are specified by executable name and version number that are acceptable.

14. The method of claim 12, wherein said applications are specified by digital signatures that are acceptable.

15. The method of claim 14, wherein said digital signatures are computed using a cryptographic hash.

16. The method of claim 15, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

17. The method of claim 1, wherein said access policy specifies Internet access activities that are permitted or restricted for applications or versions thereof.

18. The method of claim 1, wherein said access policy specifies rules that are transmitted to client computers from a remote location.

19. The method of claim 18 wherein said remote location comprises a centralized location for maintaining said access policy.

20. The method of claim 1, wherein said blocking step includes:

determining, based on identification of a particular client computer or group thereof, a specific subset of rules filtered for that particular client computer or group thereof.

21. The method of claim 1, wherein said challenge includes a request for a particular client computer to respond as to whether it is in compliance with said access policy.

22. The method of claim 1, further comprising:

redirecting a client computer that is not in compliance with said access policy to a sandbox server; and

informing such client computer that it is not in compliance with said access policy.

23. The method of claim 22 further comprising:

redirecting a client computer that is not in compliance with a particular access policy, to a particular port on the sandbox server; and

displaying particular error message pages on the sandbox server in response to communications on particular ports.

24. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:

transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy;

transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued; and

redirecting a request for Internet access by any client computer that does not respond appropriately to said challenge to a sandbox server.

25. The method of claim 24, further comprising:

displaying an error message on the sandbox server to any client computer that does not respond appropriately to said challenge.

26. The method of claim 25, further comprising:

after display of such error message, permitting said client computer to elect to access the Internet.

27. The method of claim 24, wherein a client computer that responds with a particular predefined code indicating non-compliance is redirected to said sandbox server.

28. The method of claim 24, wherein a client computer that responds with a particular predefined code indicating compliance is permitted Internet access.

29. The method of claim 24, further comprising:

before receipt of a challenge, transmitting an initial message from a particular client computer to the client premises equipment, for requesting the client premises equipment to transmit a challenge to that particular client computer.

30. The method of claim 29, wherein said initial message comprises a "client hello" packet.

31. The method of claim 24, wherein said client premises equipment is capable of permitting Internet access by selected client computers and redirecting other client computers to the sandbox server.

32. The method of claim 24, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

33. The method of claim 24, wherein said access policy specifies which applications are allowed Internet access.

34. The method of claim 24, wherein said access policy specifies executable names and version number of applications that are allowed Internet access.

35. The method of claim 24, wherein said access policy specifies Internet access activities that are permitted or restricted for applications or versions thereof.

36. The method of claim 24, wherein said access policy specifies rules that are transmitted to client computers from a remote location.

37. The method of claim 36, wherein said remote location comprises a centralized location for maintaining said access policy.

38. The method of claim 24, wherein said step of redirecting a client computer includes:

determining, based on identification of a particular client computer or group thereof, a specific subset of rules filtered for that particular client computer or group thereof.

39. The method of claim 24, wherein said challenge includes a request for a particular client computer to respond as to whether it is in compliance with said access policy.

40. The method of claim 24, further comprising:

redirecting a client computer that is not in compliance with a particular access policy, to a particular port on the sandbox server; and

displaying particular error messages on the sandbox server in response to communications on particular ports.

41. The method of claim 24, further comprising:

permitting client computers that are not in compliance with particular access policies to elect to access the Internet; and

blocking computers that are not in compliance with other access policies from accessing the Internet.

42. The method of claim 24, wherein said applications are specified by digital signatures that are acceptable.

43. The method of claim 42, wherein said digital signatures are computed using a cryptographic hash.

44. The method of claim 43, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

45. A system for regulating Internet access by client computers comprising:

an access policy governing Internet access by said client computers;

client premises equipment serving a routing function for each client computer to be regulated and capable of issuing a challenge to each client computer, for determining whether a given client computer is in compliance with said access policy;

one or more client computers which can connect to the Internet and at least one of which can respond to challenges issued by said client premises equipment; and

an enforcement module for selectively blocking Internet access to the Internet to client computers not in compliance with said access policy.

46. The system of claim 45, wherein said client premises equipment includes a router.

47. The system of claim 45, wherein said access policy is provided at each client computer to be regulated.

48. The system of claim 45, wherein said enforcement module is provided at said client premises equipment.

49. The system of claim 45, wherein said at least one client computer capable of respond to challenges can respond with a particular predefined code indicating noncompliance with said access policy is blocked from Internet access.

50. The system of claim 49, wherein a client computer that responds with a particular predefined code indicating compliance with said access policy is permitted Internet access.

51. The system of claim 45, wherein at least one of the client computer is capable of transmitting an initial message to the client premises equipment before receipt of a challenge, for requesting the client premises equipment to transmit a challenge to that particular client computer.

52. The system of claim 45, wherein said enforcement module is capable of permitting Internet access by selected client computers and denying access to other client computers.

53. The system of claim 45, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

54. The system of claim 53, wherein said enforcement module is capable of determining, based on identification of a particular client computer or group thereof, a specific subset of said access policies filtered for that particular client computer or group thereof.

55. The system of claim 45, wherein said access policy specifies applications that are allowed Internet access.

56. The system of claim 55, wherein said applications are specified by executable name and version number that are acceptable.

57. The system of claim 55, wherein said access policy specifies types of activities which applications are allowed to perform or restricted from performing.

58. The system of claim 55, wherein said applications are specified by digital signatures that are acceptable.

59. The system of claim 58, wherein said digital signatures are computed using a cryptographic hash.

60. The system of claim 59, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

61. The system of claim 45, further comprising:

a sandbox server to which client computers that are not in compliance with said access policy are redirected.

62. The system of claim 61, wherein said sandbox server informs non-compliant client computers that they are not in compliance with said access policy.

63. The system of claim 62, wherein said client computers client computers may elect to access the Internet after being informed that they are not in compliance with said access policy.

64. The system of claim 61, wherein:

said enforcement module is capable of redirecting a client computer that is not in compliance with a particular access policy to a particular port on the sandbox server; and

said sandbox server is capable of displaying particular error message pages in response to communications on particular ports.